CrossTalk would like to thank DHS for sponsoring this issue.

This sponsor's note is from a discussion with **Joe Jarzombek** *sharing his perspectives on advancements in software supply chain assurance relative to enterprise risk management and user safety and security.*

With the Internet of Things (IoT) enabling a cyber-reliant world of connected devices and products, many enterprises and informed buyers have begun to demand that those products be evaluated from a perspective of enterprise resilience and consumer protection, especially since much of IoT in enabled and controlled by third-party open source software. Safe and secure use of cyber assets places responsibilities on operators and users; yet realization of cyber assurance requires more focus on cyber 'hygiene' in the supply chain. It requires network-connectable devices to be developed and deployed with cyber-physical security and safety in mind. IoT devices need to be patchable to be responsive to a changing threat environment, and before being deployed, they should be independently evaluated not to possess exploitable weaknesses, known vulnerabilities, and malware.

The U.S Digital Service and General Services Administration's 18F have been big proponents of open source. The Office of Management and Budget (OMB) is launching "Code.gov" to give agencies more tools and best practices to help implement the 8 Aug 2016 open source policy. Code.gov will eventually serve as an inventory of all of agencies' open and accessible code. Hopefully, the open source software (OSS) that will be made accessible to all agencies will be evaluated not to possess exploitable weaknesses, known vulnerabilities, and malware. To be of real utility, the OSS will need a bill of materials such that those reusing the OSS assets can operationally respond to changing threat environments in which software has become a favorite vector of attack.

National Institute of Standards and Technology (NIST) Special Pub 800-161 provides guidance and security controls for Supply Chain Risk Management (SCRM), and NIST SP 800-160 Systems Security Engineering, Appendix J 'Software Security and Assurance' provides controls, consistent with SP 800-53, that include architecture choices, design choices, added security functions, activities and processes, code assessments, design reviews, and various types of testing. NIST SPs are provided for voluntary adoption; yet more of those controls are now specified in government policies, directives, and contracts; thus making those controls mandatory for procured and deployed products, systems and services.

Cybersecurity professionals within DoD and the intelligence community already understand these controls are not optional, and that they need skills to accomplish or oversee the implementation of these controls. The Committee for National Security Systems (CNSS) Instruction 1253 and Director of Central Intelligence Directive (DCID) 6/3 have provided precursors for the transition to Intelligence Community Directive (ICD) 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation." With the transition from DCID 6/3 to the Risk Management Framework (RMF), cybersecurity practitioners need to understand available options in terms of relevant security control families, and common/hybrid/system-specific security controls; tailoring and the identification of control enhancements. Practitioners need to implement security controls in the System Development Life Cycle (SDLC) and through operational continuous monitoring.

The unfortunate reality has been that many cyber assets have been procured without requisite security controls and without a bill of materials to indicate the composition or content of third-party open source software that enables and controls assets vital in critical infrastructure operations. That makes it extremely difficult for cybersecurity professionals to secure those exploitable assets after procurement. As a minimum, cybersecurity professional need products that have been evaluated to determine they do not have malware, known vulnerabilities and software security weaknesses. This includes relevant test and certification activities that focus on mitigating exploitable weaknesses that could have otherwise been vectors of future zero-day exploits, if not mitigated prior to use. IoT trust can be enabled with verification and validation activities focused on quality, safety, and security of devices in the context of the environments in which they would be used.

Fortunately for consumers, many white-hat researchers and test labs are equipped with tools and methods that provide third-party analysis of IoT products relative to cyber-physical security and safety. Underwriters Laboratories (UL) launched its Cybersecurity Assurance Program in April 2016 (addressing the needs stated above), and UL has already started putting its certification mark on network-connectable systems and IoT products, such as industrial control systems. These efforts provide better synergy between cyber assurance and cyber insurance since both provide a focus for mitigating residual risk.

Many tools are available to detect and aid in mitigating known vulnerabilities (CVEs), exploitable weaknesses (CWEs) and malware. The fact that new products are still being released with known vulnerabilities and weaknesses causes many to question the cyber hygiene of those in the supply chain. Why are users left to find those exploitable flaws and mitigate or patch those products when developers could/should have mitigated those risks prior to delivery or as part of a product release update? Why do suppliers not provide a bill of materials for third party OSS that would enable using enterprises to identify newly reported CVEs? The answers seem to revolve around the fact that suppliers have no liability associated with products tainted with malware, known vulnerabilities and weaknesses; so what are their motivations to address those flaws in the supply chain prior to putting users at risk?

'Enterprise/consumer demand' specified in terms of procurement language in contracts is making a difference. The DoD Software Assurance Community of Practice (CoP) has drafted sample contract language, and the "2016 Cyber Insurance Buying Guide," published by the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, provides supply chain cyber assurance procurement requirements. More sectors are developing exemplar procurement language; pushing demand signals for properly tested products with bill of materials to enable responses to changing threat environments.

It seems supply chain assurance can best be achieved with consumer demand via contracts and through adoption of independent evaluation and certification of IoT products because realization of risks attributable to known vulnerabilities and weaknesses are primarily on the use side; not the supply side. Cyber insurance is leveraging this relationship with cybersecurity assurance practices for IoT products.

Joe Jarzombek *has been involved with CrossTalk for over two decades. He previously served Director for Software and Supply Chain Assurance in the US Department of Homeland Security. Having retired from both DHS and DoD, he is now serving as Global Manager for Software Supply Chain Management in the Synopsys Software Integrity Group. He continues to collaborate on addressing software assurance, supply chain risk management, and security automation initiatives to enable scalable information sharing among organizations and security researchers. He freely shares SwA/SCRM best practices and resources, such as procurement language. He can be reached via* **joe.jarzombek [at] synopsys.com .**